CLAIMS

What is claimed is:

1. A method comprising:

generating an attestation key pair within a platform; and

producing a certificate including a public attestation key to attest that a private attestation key, corresponding to the public attestation key, is stored in hardware-protected memory.

2. The method of claim 1, wherein prior to generating the attestation key pair, the method further comprises providing the platform including a processor and a system memory including an isolated area accessible only by the processor running in an isolated execution mode.

3. The method of claim 1, wherein the producing of the certificate occurs at an initial power-on of the platform.

4. The method of claim 2, wherein the producing of the certificate comprises:

booting the platform from code stored in a platform readable medium loaded by an agent; and

executing an applet running within the isolated area of the system memory to generate the attestation key pair.

5. The method of claim 4, wherein the producing of the certificate further comprises encrypting the public attestation key with a private key held by the agent.

6 The method of claim 1, wherein the producing of the certificate comprises:

encrypting the public attestation key using a private key held by an original equipment manufacturer of the platform.

7 The method of claim 1 further comprising:

receiving a challenge message from a remotely located platform, the challenge message including a nonce.

8 The method of claim 7 further comprising:

generating a response message for transmission to the remotely located platform, the response message including the certificate, the nonce and a hash value of an audit log.

9 The method of claim 8, wherein the nonce and the hash value are signed with the private attestation key.

10. A platform comprising:

a processor to operate in one of a normal execution mode and an isolated execution mode;

an input/output control hub in communication with the processor, the input/output control hub to generate an attestation key pair and to store an audit log being a listing of data representing a plurality of software modules loaded within the platform.

11 The platform of claim 10, wherein the plurality of software modules include a processor nub and an operating system nub.

12. The platform of claim 10 further comprising at least one input/output device allowing communications with a remotely located platform.

13. The platform of claim 10 further comprising a token link coupled to the input/output control hub, the token link providing a communication path for a token.

14. The platform of claim 13 wherein the token stores a private attestation key of the attestation key pair.

15. A platform comprising:

a processor to operate in either a normal execution mode or an isolated execution mode;

a system memory coupled to the processor, the system memory including an isolated area and a non-isolated area;

a device in communication with the processor, the device to store an audit log, the audit log being a listing of data or presenting information loaded into the isolated area of the system memory; and

a token to generate an attestation key pair to load at least a private attestation key of the attestation key pair into a protected memory.

16. The platform of claim 15, wherein the protected memory includes a plurality of single write, multiple-read control registers.

17. The platform of claim 15, wherein the device is an input/output control nub.

18. The platform of claim 15, wherein the token further generates an attestation certificate to attest that the private attestation key is stored in protected memory.

19. A method comprising:

generating an attestation key pair;

storing a private attestation key into hardware-protected memory; and

producing a certificate including the public attestation key to attest that the private attestation key is stored in the hardware protected memory.

20. The method of claim 19, wherein the hardware-protected memory includes single-write, multiple-read control registers.

21. The method of claim 19, wherein the hardware-protected memory includes an isolated area of a system memory accessible to a processor when operating in an isolated execution mode.

22. The method of claim 19, wherein the producing of the certificate occurs at an initial power-on of the platform.

23. The method of claim 19, wherein the producing of the certificate comprises:

booting a platform including the hardware-protected memory from code stored in a readable medium loaded by an agent; and

executing an applet stored in the hardware-protected memory to generate the attestation key pair.